

PROJECT REPORT

ON

CYBER SECURITY: PREVENTING ATTACKS ON WEBSITES,

A CASE STUDY OF

MYBOOKSANDSTAIONARY.COM AND LABONEEXPRESS.COM

Submitted by

MAWULI AGBOKLU

(300621320879)

In partial fulfillment for the award of the degree

Of

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

B.Sc. (IT)

## **DECLARATION**

I hereby declare that the project work titled “CYBER SECURITY, PREVENTING ATTACKS ON WEBSITES, CASE STUDY OF MYBOOKSANDSTATIONARY.COM AND LABONEEXPRESS.COM” submitted to BLUECREST COLLEGE, is a record of an original work done by me under the supervision of MR. SETH ALORNYO faculty member, department of technology at BLUECREST COLEGE, and this project work is submitted in partial fulfillment of the requirements for the award of the degree of bachelor of science in information technology. The results embodied in this project work has not been submitted to any other university or institute for the award of any degree or diploma.

Student Signature

(300621320879)

## **CERTIFICATE**

This is to certify that, the project work entitled “CYBER SECURITY, PREVENTING ATTACKS ON WEBSITES, CASE STUDY OF MYBOOKSANDSTATIONARY.COM AND LABONEEXPRESS.COM” submitted by MR. MAWULI AGBOKLU for the partial fulfillment of the BACHELOR OF SCIENCE DEGREE IN INFORMATION TECHNOLOGY offered by BLUECREST COLLEGE, GHANA, affiliated to the UNIVERSITY OF EDUCATION Winneba during the 2016-2017 academic year is an original work done by the student under my supervision, and this work has not formed the basis for the award of any Degree, Diploma or such other titles.

Signature of the Supervisor

Name: Mr. Seth Alornyo

Date:

Signature of Programme Co-ordinator

Name: Mr. Charles Saah

Date:

Signature of Associate Dean (Academics)

Name: Dr E. Balamurugan

Date:

## **ACKNOWLEDGEMENT**

I have taken efforts in this project. However, it would have been impossible without the help and support of some individuals. I would like to extend my sincere gratitude to them.

I am greatly indebted to ISAAC GBEDZE, GEORGE AGBOKLU, EYRAM AMEDZOR and many others for the guidance, support and constant supervision of the project as well as providing me with relevant information in completing this project.

Finally, I would like to thank my project supervisor and other project supervisors for their constant guidance and direction in completing the project. I'm forever grateful.

## **ABSTRACT**

Security in the cyber space is very important. As the world leverages the opportunities the World Wide Web presents to simplify everyday tasks, the security of data given out by customers who patronize e-commerce websites and any other website that requires personal information is as important as keeping trade secrets. This project is a case study that studies two different websites with the aim of accessing the cyber vulnerabilities they are exposed to and how they can be prevented or mitigated. The goal of this project is to identify cyber-attacks that websites are susceptible to and how they can be prevented or mitigated.

## LIST OF IMAGES

FIGURE 1. HIGH VULNERABILITIES.....	27
FIGURE 2. MEDIUM VULNERABILITIES.....	31
FIGURE 3. LOW VULNERABILITIES.....	35
FIGURE 4. INFORMATIONAL VULNERABILITIES..	40
FIGURE 5. MEDIUM VULNERABILITY.....	49
FIGURE 6. LOW VULNERABILITY.....	50

## **LIST OF ACRONYMS**

SQL Structured Query Language

SQLi Structured Query Language Injection

HTML Hypertext Markup Language

DOS Denial of Service

## TABLE OF CONTENTS

DECLARATION .....	2
CERTIFICATE.....	3
ACKNOWLEDGEMENT.....	4
ABSTRACT.....	5
LIST OF IMAGES.....	6
LIST OF ACRONYMS .....	7
TABLE OF CONTENTS .....	8
CHAPTER ONE .....	10
INTRODUCTION.....	10
1.1 BACKGROUND OF STUDY .....	10
1.2 PROBLEM STATEMENT .....	12
1.3 RESEARCH QUESTION .....	13
1.4 OBJECTIVES OF THE RESEARCH .....	13
1.5 SCOPE OF RESEARCH .....	14
1.6 SIGNIFICANCE OF STUDY.....	15
CHAPTER TWO .....	16
LITERATURE REVIEW .....	16
2.1 INTROUCTION .....	16
METHODOLOGY .....	25
3.1 INTRODUCTION.....	25



<b>3.2</b>	<b>METHODOLOGY .....</b>	<b>25</b>
<b>3.3</b>	<b>SAMPLING .....</b>	<b>25</b>
<b>3.4</b>	<b>SOURCES OF DATA .....</b>	<b>26</b>
<b>3.5</b>	<b>DATA ANALYSIS .....</b>	<b>26</b>
<b>CHAPTER 4.....</b>		<b>27</b>
<b>FINDINGS .....</b>		<b>27</b>
<b>4.1 INTRODUCTION.....</b>		<b>27</b>
<b>4.2 THE FINDINGS.....</b>		<b>27</b>
<b>CHAPTER 5.....</b>		<b>56</b>
<b>5.1 INTRODUCTION.....</b>		<b>56</b>
<b>5.2 SUMMARY .....</b>		<b>56</b>
<b>5.3 CONCLUSION .....</b>		<b>57</b>
<b>5.4 RECOMMENDATION.....</b>		<b>62</b>
<b>5.5 LIMITATIONS OF THE STUDY.....</b>		<b>66</b>
<b>5.6 SUGGESTION FOR FURTHER STUDIES .....</b>		<b>66</b>
<b>REFERENCES.....</b>		<b>68</b>

# **CHAPTER ONE**

## **INTRODUCTION**

### **1.1 BACKGROUND OF STUDY**

A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer), that compromises the confidentiality, integrity or availability of the computer or information stored on it (Practical Law Company, 2011).

There are various types of cyber-attacks that are deployed to do different things. Malware injection, phishing, social engineering, brute force attacks, distributed denial of service, direct hack are a few of them.

The demand for a simple and easy life coupled with the desire to leverage the opportunities the web presents has forced a lot of activities to the web environment. Businesses in the services sector are the ones leading the change, providing their traditional services to customers online and giving them a new experience. Nonetheless, websites must maintain the AIC triad – availability, integrity and confidentiality. Websites must be available to users round the clock and globally to serve users regardless of the time and location. There must be integrity of data i.e. personal identifiable information which are submitted to the website by users in the process of accessing the web services and there must be confidentiality of these details so as they do not get into the custody of unauthorized persons.

E-commerce website eBay in a post on their official blog admitted that, there was a cyberattack on the company's local network which compromised a database containing customers' encrypted passwords, email, physical address, phone number and date of birth (ebay, 2014). According to the business insider publication, 145million eBay customers were affected in the breach (Seetharaman, 2014). Later in September of 2014, an ebay user discovered there was an XSS attack which redirected users who click on items listed by attackers through the XSS script to phishing sites designed to phish or steal usernames and passwords or send malwares to users' computers and other devices they use to access the auction site (Cluely, 2014).

Sony pictures entertainment, a subsidiary of Sony entertainment incorporated with global operations in motion picture production, television production, digital content production and distribution etc., in 2011, Sony had their website hacked by some cyber attackers exposing more than one million passwords of users stored in plaintext, 75000 music codes and 3.5 million music coupons were also uncovered through the hack (Westaway, 2011).

In May of 2011, PBS, the American public television station's website was hacked by a group of hackers; LulzSec after watching a frontline documentary on WikiLeaks which they disagreed with. The hackers defaced the PBS newshour website and exposed the websites login credentials (Mirkinson, 2011).

Fox news was also hacked through a PHP script planted by the hackers on fox.com which allowed them gain unauthorized access to the passwords of emails and twitter accounts of over 300 fox employees and associates. They tested the passwords with other sites and 16

of the affected employees used the same passwords for their LinkedIn profiles, they also hijacked the twitter accounts of two fox affiliates FOX UP and FOX 15 (Bershad, 2011).

The examples above are a few of the many cyber-attacks deployed to malfunction websites and extract vital information from them. These attacks depending on their scale and magnitude and the also the victims cost a lot to repair. The damages range from lost in customer share, to decline in share value, possible fines, potential litigation etc.

According to IBM X- Force intelligence report 2016, Malwares, DDoS, Misconfigurations, Phishing, Brute force, Malvertizing and SQL injection are some of the most common attack types being deployed in the cyber space by attackers in 2015 and some of the most commonly attacked industries are computer services, retail, healthcare, media and entertainment, financial markets, travel and transportation. The report also revealed there were physical impacts of the cyber-attacks on individuals and corporate bodies; from suicide by attempted victims to grounding of services.

## **1.2 PROBLEM STATEMENT**

It is the desire of every business small, medium or large to be able to take advantage of the many opportunities the web provides today without suffering from any form of cyber-attack. However, this ideal is far from the reality. There has been cyber-attacks on different businesses in the web environment with different magnitude of effects. This creates the need for a study into some of the vulnerabilities being exploited by cyber attackers and how these vulnerabilities can be blocked to mitigate the occurrence of cyber-attacks on businesses.

### **1.3 RESEARCH QUESTION**

The research aims at finding out the type of cyber-attacks websites are susceptible to and what prevention and mitigation measures website administrators should take to keep their websites and patrons safe from cyber criminals by providing answers to the following questions

1. What type of attacks are websites most susceptible to?
2. What will be the extent of damage to the organization if the susceptibilities are exploited by cyber criminals?
3. What are the prevention and mitigation measures available for implementation?
4. What is the best approach for website administrators to take in keeping their websites safe?

By providing answers to the above questions, the study hopes to provide solutions to website administrators on how to keep their websites secured and protect patrons' details and also enlighten them on the reality of cyber-attacks.

### **1.4 OBJECTIVES OF THE RESEARCH**

The study aims to investigate and understand the types of cyber-attacks websites are susceptible to and their prevention and mitigation measures because of the following objectives

1. To help draw the attention of website administrators to the reality of cyber-attacks.
2. To help explore the dangerous effects cyber-attacks on websites have on the website patrons.

3. To serve as a learning curve to other website administrators and organizations about cyber-attack prevention and mitigation on their websites.

## **1.5 SCOPE OF RESEARCH**

The scope of the research is a case study which can be researched in reasonable time period with available resources for relevant outcomes. The research limits itself to the subject of cyber-attacks which has increasingly taken root in the information technology domain. According to the 2015 cost of data breach study: global analysis by ponemon institute, may 2015, the average cost paid for each lost or stolen record containing sensitive and confidential information increased from \$145 in 2014 to \$154, which goes to imply that, cyber-attacks are becoming expensive to fix or remediate.

The case study involves two websites which are providing two different services within the e-commerce and magazine business environment and findings of the study are peculiar to these websites but could however, be suggestive of what is found on other websites.

Furthermore, Ghana is an opening economy with growing prospects and an increasing population of technology upbeat individuals and businesses which means more activities in the Ghanaian cyber space hence the need for cyber-attack awareness and vigilance.

In summary, the scope of the study is to identify cyber-attacks websites are susceptible to and the prevention and mitigation measures websites administrators can take to keep their websites and patrons safe.

## **1.6 SIGNIFICANCE OF STUDY**

This research will enlighten us on vulnerabilities within websites which are exploited by attackers to launch cyber-attacks and this will inform information technology professionals; mostly website administrators of the different types of attacks websites are susceptible to which the study hopes should inform their security decisions as well as general procedure decisions.

Businesses loose time and money when these attacks occur therefore, the research seeks to contribute to efforts to help prevent these attacks to save time and money. Individuals who patronize websites are not exempted from the dangers cyber-attacks pose hence the study also seeks to educate individuals on how to be secured in the cyber space.

This study can be a head start for any subsequent research which will study in-depth any of the types of attacks and provide in-depth solution to it. This study will also serve as a learning curve to organizations and individuals that may come into contact with it.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1 INTROUCTION**

Cyber-attacks have been widespread across the information technology domain; mostly web applications and websites. Security experts have investigated these cyber-attacks on different industries and have arrived at various outcomes which have been analyzed and reported in annual security reports.

One key observation from the researches is that, successful cyber-attacks have damaging effects and the victims cut across; from businesses to individuals to social groupings. The motives behind this attacks is one aspect that has been (faintly) addressed by researches. It has however been noticed that, whiles some of the attacks are purely financially motivated, others are ideologically motivated.

This chapter presents reviews of existing research relevant to cyber-attacks on websites. To this end, the chapter starts with how increasingly expensive it has become fixing cyber-attacks that occur, it further goes on to examine the severity of some types of the attacks and finally reviews the responds to cyber-attacks by information technology professionals when they have been successfully launched.

“According to our research, the average total cost of a data breach for the 350 companies participating in this research increased from 3.52 to \$3.79 million<sup>2</sup>. The average cost paid for each lost or stolen record containing sensitive and confidential information increased from \$145 in 2014 to \$154 in this year’s study”. (Ponemon Institute, 2015). The study



shows that in a space of one year, there has been a phenomenal increase in the cost of data which has been breached through a vulnerability which could have taken less to fix. This cost sucks away resources from businesses because, the financial commitments which will be driven towards redeeming loss or stolen records could be directed at core business duties to shore up the growth of these businesses.

As reported by the recent IBM/ Ponemon data breach study, healthcare data breaches cost organizations significantly more than any other industry, as much as USD363 per record compromised, compared to the average for all types of data of USD154. (IBM, 2016). Cyber criminals who are financially motivated will target health care delivery organizations. Because health care is critical to human beings and has personal identifiable information (PII), attackers are more likely to exploit the vulnerabilities that may exist in their systems especially web based systems to extract the PII's for which they can make huge monetary demands. In the event that they are successful, these organizations may give in to their outrageous demands in order to protect their clients, a cost which may be later passed on to the services offered.

Online fraud impacted real-world markets when it came to light that attackers who infiltrated public relations news sites over a five-year period had made more than USD100 million using insider information gleaned from soon-to-be-published corporate press releases. In addition to suffering breached payment systems, the travel industry felt physical impacts of cyber-attacks, as seen in the case of a Polish airline. In June, flights were grounded in Warsaw by what was believed to be a DDoS attack that disrupted flight plan computer systems and prevented access to data necessary for departures. (IBM, 2016). This is are very damaging consequences of cyber-attacks businesses are exposed

to and this is how much it costs if there are vulnerability in online systems and they are constantly overlooked. On a very bad occasion when an attacker launches a successful incident, the whole online service will grind to a halt and money lost would be far greater than what could be used in fixing the vulnerability. Every passing day that a vulnerability exists in a system the more costly it gets.

Conventional web attacks from XSS and SQLi rose by 200% and 150% respectively continuing the trend from last year, with larger numbers and larger volumes of scanning campaigns across the Internet (Imperva, 2015). XSS (Cross Site Scripting) and SQLi (SQL Injection) are one of the most severe attack vectors any cyber attacker can deploy to gain access to target systems and exploit vulnerabilities. These two vectors are in the OWASP (Open Web Application Security Project) top 10 vulnerabilities list and increase in their use goes to show their proficiency.

By leveraging an SQL injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL injection can also be used to add, modify and delete records in a database, affecting data integrity. To such an extent, SQL injection can provide an attacker with unauthorized access to sensitive data including, customer data, personally identifiable information (PII), trade secrets, intellectual property and other sensitive information. (Acunetix, 2016).

Databases are a crucial component of websites and web applications. They hold information about users and other business sensitive information. Information like trade secrets and intellectual properties are stored in databases in order to maintain their integrity. When these databases become susceptible to vulnerabilities like SQL injection,

the whole business is at risk. SQL injection can provide an attacker a complete access to the target which can allow him manipulate the database like deleting columns or rows or tables. This will dent the integrity of whatever information the legitimate owners of the database may try to generate using data from the database because, they might either be working with a truncated data or bloated data.

23% of sampled targets were vulnerable to at least one SQL injection vulnerability. The severity and ease of exploitation, combined with the maturity of exploitation tools targeting SQL injection makes this figure worrying; especially when considering how well understood and documented this vulnerability is. (Acunetix, 2016). SQL injection is a major security threat to websites and web applications.

Half of the applications analyzed were the target of more than 20 SQLi attacks within a six-month period. In terms of attack magnitude, the typical SQLi attack included 72 malicious requests, with the most intensive SQLi attack detected by our sensors amounting to 400,000 malicious requests. (Imperva, 2015). The statistics show that attackers are finding SQL injections as an efficient vector and they are increasingly deploying it to exploit website and web application vulnerabilities.

While SQL Injection is mostly used to steal data from the database, an SQLi vulnerability can easily be escalated further if the permissions on the database are incorrectly configured. For example, the attacker can inject a query that causes some tables to be deleted from the database, effectively causing a DOS attack. The attacker can also take over the server hosting the database using Remote Code Execution (RCE) by constructing SQL queries that execute code on the database server (Acunetix, 2015).

Since an SQL injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities. (Acunetix, 2016).

The proficiency of SQL injection has made it a prime vulnerability for remediation by website administrators to keep their domains and customer details safe.

Cross site scripting is vulnerability exploit users the most. According to acunetix, 33% of sampled targets were vulnerable to at least one Cross-site Scripting vulnerability. The combination of XSS and social engineering, allow attackers to pull off advanced attacks including cookie theft, keylogging, phishing and identity theft. Critically, XSS vulnerabilities provide the perfect ground for attackers to escalate attacks to more serious ones. (Acunetix, 2016).

Healthcare web applications suffer substantially more XSS attacks than other sectors. When excluding SPAM and RCE, 57% of the attacks are XSS, significantly more than other sectors. The average number of XSS attacks in the healthcare sector is almost 10 times higher than the other industries. Healthcare is possibly attractive for hijacking sessions through XSS, for the sake of stealing Personal Identifiable Information (PII). (Imperva, 2015). Attackers choose their victims carefully. They try to choose the most vulnerable victims and exploit them to the maximum they can. The increase in attack on healthcare websites and web applications is that, they contain personally identifiable information (PII) of patients. No patient would want their medical details to be subject to public scrutiny especially patients with high public status like politicians and entertainers so, if attackers gets lucky through an attack and have details of such personalities, they could be exploited for the rest of their lives.

Most of the websites developed in recent times use content management systems like WordPress and Drupal. However, the safety of these websites cannot be guaranteed. (IBM, 2016), As developer tools and frameworks become easier to implement, the barriers end users face when creating scalable applications and websites drop. With reduced barriers to entry, more less-experienced developers enter the fray, and the risks of unsafe development increase. For consumers, it is worth remembering that the fact that an application is popular or has millions of users does not mean it is safe. Most of the developers are concerned with the aestheticity of the webpages and relegate the issues of security to the background.

CMS applications suffer on average three times more attack incidents than non-CMS applications, with 3,049 attack incidents in the report period, compared to only 1,010 incidents for non-CMS applications. This trend holds for essentially all attack types. WordPress applications suffer from even more attacks, with 3,497 attack incidents in six months—250% more than non-CMS applications. (Imperva, 2015).

Because of the popularity of web content management systems amongst web developers, (Wikipedia, 2016), Based on market share statistics, the most popular content management system is WordPress, used by over 27% of websites on the internet. The attention of attackers have been drawn to these content management systems to exploit security vulnerabilities. We found that WordPress was attacked 3.5 times more often than non-CMS applications. (Imperva, 2015).

Even though some content management systems are putting in their best efforts to remain safe, there is still much work to do and until these loopholes are covered, attackers will continue to attack websites developed with content management systems as frequently as

they can. “While there are some inherent security weaknesses in WordPress’ defaults, such as username enumeration, and XML-RPC authentication bruteforcing, the WordPress community strives to make security a priority, especially with automatic security updates turned on by default. Arguably the opposite can be said for the CMS’ vibrant plugin and theme ecosystem”. (Acunetix, 2016).

Most websites and web applications frequently leverage one or more JavaScript libraries to enhance the user experience of the site, as well as to build core functionality of the web application. Running vulnerable versions of JavaScript libraries such as jQuery, jQuery UI, YUI, PrototypeJS, EmberJS and Dojo are inherently at risk of Cross-site Scripting vulnerabilities present in the vulnerable versions of those frameworks (Acunetix, 2015)

Malware advertising is another vector which can be deployed to take hold of target systems. “Malicious advertising increased throughout 2015. In these cases, infected ads, primarily targeting Adobe Flash vulnerabilities, were served to millions of viewers on popular websites and resulted in the installation of ransomware and other types of malware”. (IBM, 2016).

Attackers with successful malwares install malicious software on the compromised systems and demand financial rewards from victims before the systems are unlocked. Attackers will often compromise a Web site by exploiting site-specific vulnerabilities and then use that site to launch shotgun attacks to exploit browser plug-in vulnerabilities. The attacker can then install malicious software—such as Trojans, back doors, and bots—on the compromised computer. (Symantec , 2008).

The phishing vector is also a technique used by cyber attackers to deceive website users into logging in into mimicked websites created by the attackers so they can extract user login credentials and other user specific information for financial gains. A phishing Website is a site that is designed to mimic the legitimate Web site of an organization, often an online bank or e-commerce retailer, in order to fool a user into disclosing personal information associated with that organization, such as banking credentials, account information and so on. This information is usually used in fraudulent activities for financial gain. (Symantec , 2008).

Denial of Service attacks are used to prevent legitimate website users from accessing the web service. This causes business loss and adds to the cost of business. DoS attacks attempt to make a server, service or network resource unavailable to its intended users, it likely results in loss of business as well as increased resource usage, possibly resulting in extra infrastructural and data transfer costs. (Acunetix, 2016).

Detect-by-reputation alerts comprised 78% of the total number of alerts, or approximately 100,000 malicious requests that an application sees every month that were blocked without the application's involvement. (Imperva, 2015). In protecting websites and web applications from attacks detection of malicious request is important.

The time taken by website administrators to respond to cyber-attacks by patching up the vulnerabilities is slow. "Site-specific vulnerabilities are also popular with attackers because so few of them are addressed in a timely manner. Of the 11,253 site-specific cross-site scripting vulnerabilities documented during this period, only 473 had been patched by the administrator of the affected Web site. Of the 6,961 site-specific vulnerabilities in the first six months of 2007, only 330 had been fixed at the time of

writing. In the rare cases when administrators do fix these vulnerabilities, they are relatively slow to do so”. (Symantec , 2008).

Scarce resources are also a contributing factor to the slow responds by website administrators to cyber-attacks. “On average, it takes approximately 150 days to fix vulnerabilities. Critical vulnerabilities are not resolved significantly more quickly than the rest, and high-risk vulnerabilities actually take the most time to fix. This may reflect a greater level of complexity, or that when organizations have the resources to fix only some vulnerabilities, the critical vulnerabilities will be resolved first and the remainder are resolved as resources are available – with simpler fixes being performed first, regardless of the risk level”. (Whitehat Security, 2016).

The study is centered on two websites mybooksandstationary.com and laboneexpress.com which provide two different services for two different sets of users. Most recent researches on cyber-attacks have adopted both qualitative and quantitative methods which they have used to identify threat trends, measure the magnitude of damage caused by these attacks and the frequency of the vector usage by cyber attackers. However, this study adopts a qualitative research method to gain more insight into types of attacks the case studies are susceptible to, and how to prevent and mitigate them. The expectation of this research is that, useful information will be obtained to prevent and mitigate cyber-attacks on websites. This study shall also be a contribution to ongoing efforts of documentations on cyber-attacks in Ghana.



## **CHAPTER THREE**

### **METHODOLOGY**

#### **3.1 INTRODUCTION**

This chapter presents the research methodology. In the chapter, the research methodology, data collection methods and data analysis technique are presented. The basis for choosing some of the methods used in this study are also explained.

#### **3.2 METHODOLOGY**

The study adopts a case study and a qualitative research approach to methodically investigate two different websites by using two main sources of data; primary and secondary sources of data to understand the subject of study.

#### **3.3 SAMPLING**

Sampling is a set of respondents from which information is obtained for a research study. There are two main types of sampling, they are probability and non- probability sampling.

The probability sample presents every member of the population with equal opportunity of being selected as a respondent.

The non-probability sampling does not present members of the population with equal opportunity of being selected as a respondent.

The sampling for the research adopts a non-probability sampling type. Because, the research has been focused on the objectives, the sampling type ensures optimization of

available resources and time and it is best to seek information from professionals with valuable knowledge about the study area.

### **3.4 SOURCES OF DATA**

This study employs both primary and secondary sources of data collection. Primary data source collects data from the field directly whiles secondary data source collects data from other data sources like reports, books and articles. The techniques used for the primary data collection in this research are

- I. Semi- structured interviews. Semi- structured interviews allow the interviewer with the flexibility to ask broad questions. It provides the interviewer with more space to probe the respondent further to disclose more information and bring forth better understanding of the subject.
- II. Observation. This study employs observation as part of its primary source of data. Because, observing closely the operations of the case studies will offer some insight to the area of study.

The following is the technique used for the secondary source of data.

- I. Acunetix Web Vulnerability Scanner. Acunetix web vulnerability scanner will be used to test the sample websites for vulnerabilities existent on their websites that pose a risk to patrons.

### **3.5 DATA ANALYSIS**

The data analysis adopted by this research work is a deductive analysis of qualitative data. Deductive analysis is a top down approach which arrives at a conclusion reductively by applying general rules that hold, over the collected data.

## CHAPTER 4

### FINDINGS

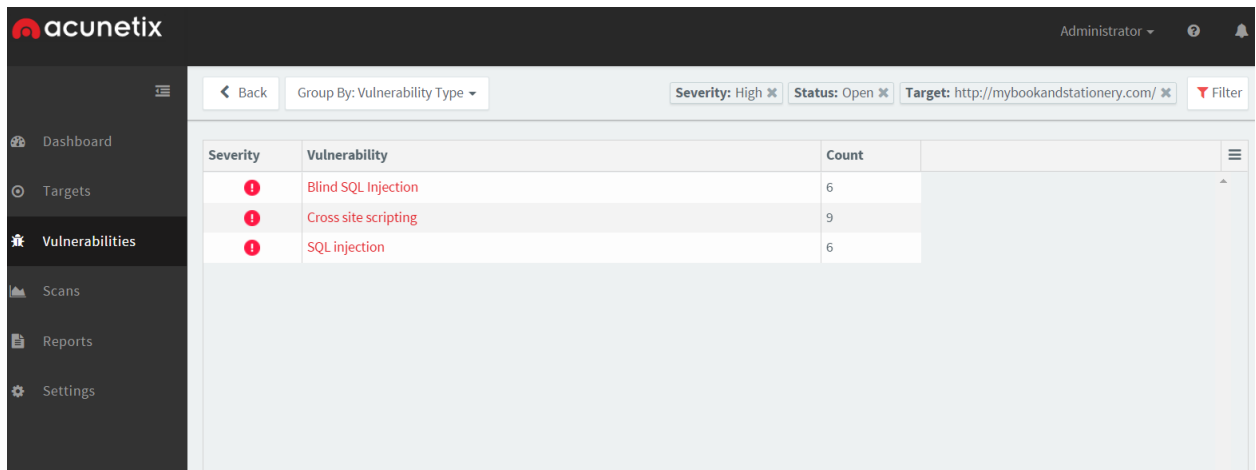
#### 4.1 INTRODUCTION

This chapter presents the findings of the study. Findings from acunetix vulnerability scan software, observation, and semi-structured interviews. Acunetix vulnerability scan has grouped the vulnerabilities into four types; high, medium, low and informational. The findings on mybooksandstationary.com are presented first and then findings from laboneexpress.com are presented second.

#### 4.2 THE FINDINGS

#### FINDINGS ON MYBOOKSANDSTATIONARY.COM USING ACUNETIX WEB VULNERABILITY SCANNER

#### ACUNETIX WEB VULNERABILITY SCANNER SNAPSHOT



The screenshot displays the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes the Acunetix logo, a user dropdown menu for 'Administrator', and notification icons. The left sidebar contains navigation links for Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area shows a table of vulnerabilities filtered by 'Severity: High', 'Status: Open', and 'Target: http://mybookandstationery.com/'. The table lists three high-severity vulnerabilities: Blind SQL Injection (6 occurrences), Cross site scripting (9 occurrences), and SQL injection (6 occurrences). Each entry is marked with a red 'H' icon indicating high severity.

Severity	Vulnerability	Count
H	Blind SQL Injection	6
H	Cross site scripting	9
H	SQL injection	6

Figure 1. High vulnerabilities. Source: Acunetix Web Vulnerability Scanner version 11.

## **BLIND SQL INJECTION**

Blind sql injection is a type of code injection attack which cyber attackers use to attack websites and get access to their databases. They use sql statements to manipulate the user input sections on websites in a bid to execute the statements in the database and manipulate it. Mybooksandstationary.com depends on a database to run the website because, the database keeps the files necessary for display on the website and also keeps user inputs from the website. The website cannot fulfil its purpose without a database at the backend.

Using the acunetix vulnerability scanner, it has been shown that, Mybooksandstationary.com is exposed to blind sql injection attack. The vulnerability resides in the sql database used by the website. Metacharacter inputs which are received from users in the creation of their accounts i.e. usernames and passwords to give their accounts a distinct name and a strong password are not being properly filtered. This type of inputs are left to infinite metacharacters without any strict filter and this is a loophole which is present within the database and can be exploited by cyber attackers immediately they find out. This vulnerability can cause user credentials like their phone numbers, account usernames and passwords and bank card details used in making purchases from the website be exposed to a third party who may use it for malicious purposes. The blind sql injection vulnerability poses a threat to the running of the entire website as any successful exploitation of the vulnerability could make a complete alteration to the database of the website by the attacker.

Blind sql injection bares similarities with normal sql injection attack to a large extent but has some differences. The difference is that, unlike the normal sql injection attack that gives a valuable error message after passing the sql statements, the blind sql injection attempts return a generic page which has been developed by the developer not to display any error messages at all or make the website unresponsive to the request in a bid combat any injection attempt. This approach conceals detailed error messages from being outputted on the website after a failed entry but does not solve the problem of the vulnerability of user inputs being parsed as sql statements. The attackers will now resolve to frame True or False i.e. Boolean expression sql statements to confirm the availability of a blind sql vulnerability and then proceed to frame payloads which can help them manipulate the user input section further to retrieve data from the database.

### **CROSS SITE SCRIPTING.**

Cross site scripting is another attack vector the website mybooksandstationary.com is expose to; according to acunetix vulnerability scanner.

Cross site scripting is in short referred to as XSS attacks. Attackers use this attack vector to inject malicious scripts into client side of vulnerable web pages which is executed by the client's browser upon opening the webpage. This malicious scripts can be very harmful to the client in that, when it is executed by the browser, it can transmit tokens, session cookies, and other browser and webpage unique information to the attackers' websites. When the XSS attack is successful and an attacker gains access to users' session cookies, the attacker could impersonate users and make orders from the website on their behalf. Users can also be redirected to a dummy page built by the attacker where they will be led to input their log in credentials again and this will be captured by the

attacker to gain access to users' original accounts on the original website. Attackers can also use the dummy pages to install Trojan programs on users' computers through which they can have access to their local files. XSS attacks can also lead to modification of page content to mislead patrons of the website.

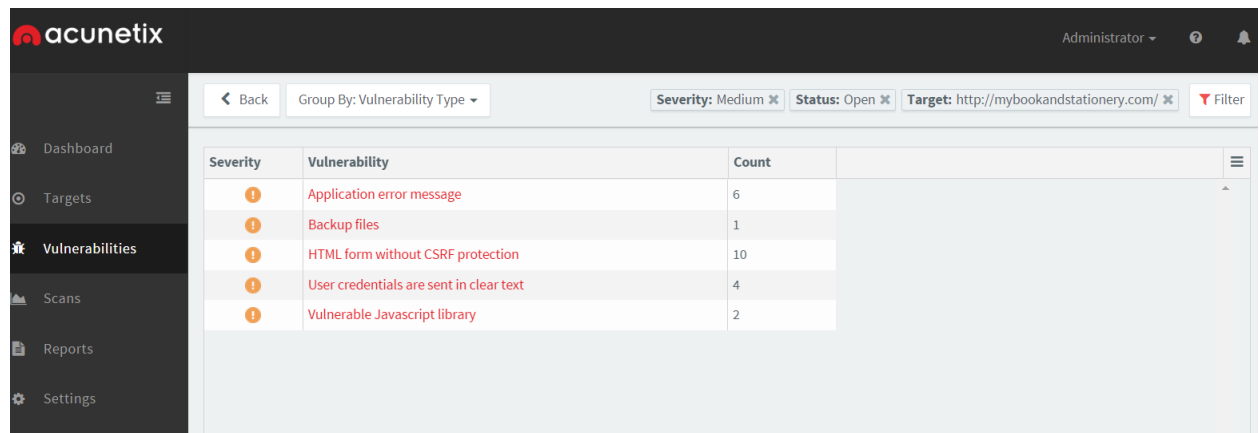
Cross site scripting has no specific target. The targets are all those who will open a webpage within a website that has this vulnerability exploited by an attacker. The scripts used in XSS attacks are usually JavaScripts. JavaScripts are used by most websites to make the website dynamic and able to interact with the user. They provide dynamism to the webpages. JavaScripts are mostly used in conjunction with HTML and CSS by developers to develop the dynamic pages. JavaScripts are executed on the client side by the web browser and this is what gives room for the exploitation by attackers.

## **SQL INJECTION.**

Sql injection is another injection attack with devastating outcomes if successful. According to the Acunetix vulnerability scanner, mybooksandstationary.com is exposed to this attack vector. sql injection involves malicious users injecting sql statements into user input fields meant for receiving other user information from the website. This is done in an attempt to cause the website to generate valid error message about the database at the backend of the website which will help the attacker to know what sql statements to frame further and output valuable data from the database. When the data is outputted, attackers can manipulate the database by way of inserting, modifying or even deleting data from the database. A successful exploitation of this vulnerability means that the database is at the mercy of the attacker. The domain is open to sql injection attack because, developers have not properly filtered the user input fields of metacharacters on

the website. Because the sample; mybooksandstationary.com is an ecommerce website with user unique information like usernames, phone numbers, passwords, bank card details etc. , attackers will want to exploit the domain for financial rewards and sql injection is a prime vector for their mission. The presence of this vulnerability does not only expose users to unwanted disclosure of their details but the company itself to a possible exploitation which will cause them sufficient funds to fix.

## ACUNETIX WEB VULNERABILITY SCANNER SNAPSHOT



The screenshot shows the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes the Acunetix logo, a user profile dropdown for 'Administrator', and a notification bell. The left sidebar contains navigation links: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area displays a table of vulnerabilities filtered by 'Severity: Medium', 'Status: Open', and 'Target: http://mybookandstationery.com/'. The table has columns for Severity, Vulnerability, and Count.

Severity	Vulnerability	Count
Medium	Application error message	6
Medium	Backup files	1
Medium	HTML form without CSRF protection	10
Medium	User credentials are sent in clear text	4
Medium	Vulnerable Javascript library	2

Figure 2. Medium Vulnerabilities. Source: Acunetix Web Vulnerability Scanner version 11.

## APPLICATION ERROR MESSAGE

Application error messages are error messages which are generated by the system in the event of an unhandled exception. Such error messages can disclose vital information such as location of a file which can aid an attacker in its exploits. An unhandled exception is when an error is not catered for by the developer by writing another set of codes to perform alternative functions if the main function fails. The absence of a handled exception will cause the system to generate its own error message and this is where the vulnerability is. Some of the situations in which an exception can be thrown by the

system is when an attacker tries to manipulate the user input section with scripts rather than the right text format. Because it is an odd input, the system will reject it and since there are no exceptions to handle malicious script inputs, the system may be forced to generate an error message.

## **BACKUP FILES**

This is a vulnerability within mybooksandstationary.com where certain backup files of the website are created in directories accessible over the web. Backup files are files created by the web developers to backup their work. Backup files are critical files since they contain scripts sources, configuration files, databases, themes, plugins, add-ons etc. The backup files are kept in the event that, should the main website be rendered offline by any form of attack which is difficult to fix in reasonable time, the website can be restored via the backup with all its latest functionalities in no time to serve anxious customers. When such files are accessible to an attacker, it gives the attacker more insight into the composition of the website since it is a duplicate of the original site and this will help it frame more advance and precise attacks to destruct normal functioning of the website. When the backup files are affected there is no more lifeline left for developers to use in restoring the website in the unfortunate event of the main website being attack.

## **HTML FORM WITHOUT CSRF PROTECTION**

According to Acunetix vulnerability scanner, mybooksandstationary.com has html forms that accept user inputs and are not protected against a CSRF (Cross Site Request Forgery) attack. There are two main forms on the website which accepts user inputs. One for creating a user account and another for making enquiries. CSRF attack is an attack vector



where malicious individuals trick a legitimate user with authorization into performing unintended actions on a website they have already been authenticated against. Attackers gain access to users account via this vulnerability. With this loophole present in the domain for study; mybooksandstationary.com, attackers can create a similar form on a malicious website with the legitimate domain as the target for the action they intend behind the form e.g. creating multiple user accounts to flood the database of the target or make a series of false enquiries. Since there are no CSRF (Cross Site Request Forgery) protection implementations, attackers can exploit the forms to append their payloads to the target server via an http request method such as the GET or POST method.

### **USER CREDENTIALS ARE SENT IN CLEAR TEXT**

According to the threat vulnerability scanner used to scan the sample (case study); user credentials which are used by patrons to login into their accounts and purchase books and stationary are sent to the database in clear text; no encryption. The user credentials which are submitted to the database by both existing and new users are sent to the database in clear text. User credentials are the unique login details i.e. usernames and passwords which is used to uniquely identify each user on the website. This is what is used to create the accounts to which charges are made in the event of purchase. With this vulnerability, an attacker can intercept the connection at a point where the credentials are sent to the database and obtain as much user credentials as he or she can. These obtained credentials can be sold by the attacker to people with malicious intents who will use them for purchases on the same site or if the user uses those same details across platforms, the malicious users will exploit it to the disadvantage of the original user. These details which comprise of email address and password are very sensitive and unique identifiers

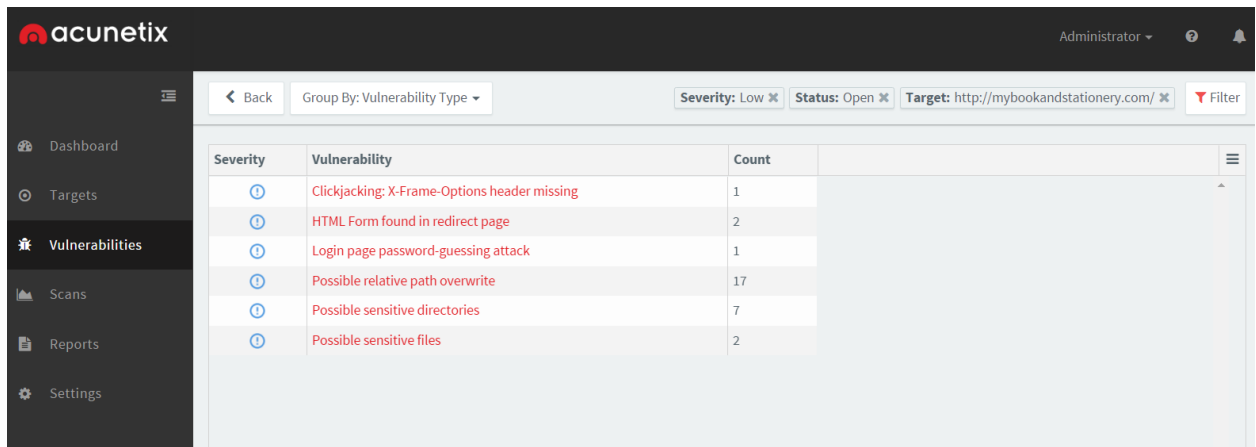
of any individual on the web and therefore, if by any chance these details are accessed by an unknown third party, users will be at great risks.

## **VULNERABLE JAVASCRIPT LIBRARY**

JavaScript is an object oriented programming language which is used to make a website dynamic and user interactive. JavaScript is executed by the client's browser and does not load as part of the website from the server. JavaScripts are used in conjunction with other web development languages like HTML (Hypertext Markup Language) and PHP (Personal Home Page) to make websites dynamic and user interactive. According to the acunetix vulnerability scanner used to scan the sample for vulnerabilities, there are vulnerable JavaScript libraries which exist within the codes. A JavaScript library is a set of prewritten JavaScript scripts to perform specific functions which are used by developers in the website development process so they do not have to write the codes all over again hence reducing the time used in development. This library is usually available with web development framework platforms like wordpress, joomla, drupal etc. because, they want to make development easier and inexpensive by providing templates for later customization by developers. Examples of JavaScript libraries are jQuery, Angular.js, react, relay and handlebars.js. JavaScripts can be run on the client side in the browser and also on the web server. The existing vulnerabilities pose great risks to end users as they can be exploited by attackers and send payloads over the web to steal user data, temper with user accounts and much more. An example of attack JavaScript vulnerabilities result in is cross-site request forgery. Cross-site request forgery is a kind of vulnerability within websites where attackers' write malicious codes into the website codes of one website to exploit a user who visits the website and is logged into his or her account on another

target website by the attacker at the same time via a browser. Cross-site request forgery also helps the attacker to determine how the target site handles authentication. The sample, being an e-commerce website will not be off the radar of attackers.

## ACUNETIX WEB VULNERABILITY SCANNER SNAPSHOT



The screenshot shows the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes the Acunetix logo, the user role 'Administrator', and a notification bell. The left sidebar contains a menu with options: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area displays a table of vulnerabilities for the target 'http://mybookandstationery.com/'. The table has columns for Severity, Vulnerability, and Count. All listed vulnerabilities are of 'Low' severity.

Severity	Vulnerability	Count
Low	Clickjacking: X-Frame-Options header missing	1
Low	HTML Form found in redirect page	2
Low	Login page password-guessing attack	1
Low	Possible relative path overwrite	17
Low	Possible sensitive directories	7
Low	Possible sensitive files	2

Figure 3. Low Vulnerabilities. Source: Acunetix Web Vulnerability Scanner version 11.

## CLICKJACKING

This is a low vulnerability identified by Acunetix vulnerability scanner. Clickjacking is a vulnerability where malicious codes are framed underneath buttons on legitimate websites to convince the user into thinking that, they are performing a particular action whereas what actually happens is that, they are directed to another page they do not intend visiting. This attack vector is used by attackers to gain access of other accounts which they believe users they might have already been authenticated against so they can use them for their malicious purposes. E.g. banking websites or some other e-commerce website. They are also use as a means to deploy malwares onto users' computers through the browser with the aim of infecting files with Trojans or locking the computer for a ransom. Clickjacking attacks are exploited against targets like

mybooksandstationary.com with a substantial amount of user traffic. This vector can further be exploited to direct users to liking pages on social media websites like Facebook or following people on twitter or tricking them to another website to click on google AdSense adds to gain pay per click revenues.

### **HTML FORM FOUND IN REDIRECT PAGE**

According to Acunetix vulnerability scanner, there is a low level vulnerability of html form found in a redirect page. Developers use redirect functionality to redirect users to the appropriate pages they request for on the website. In some instances where a user has not been authenticated, they are redirected to a login page to authenticate themselves via a username and password before accessing portions of the website which may be password protected; this is usually done for administrator portals of content management systems. However, developers most times after redirecting users do not terminate the code that checks for the user authentication and redirection. This is a vulnerability and is present in the sample of the study; mybooksandstationary.com. Knowing that, every attacker first tries to have access to the administrator's page, it is troubling to have such a vulnerability lurking in the codes for the sample. Unlike normal web browsers which will execute the redirect instruction without the user noticing there is a vulnerability, other tools such as http editors use to analyze client http requests and inspect server responses is use by attackers to craft http requests in an attempt to test their target and gather information and exploit any vulnerability they found. After returning the redirect response, text editors allows the user to browse the content of the page to which the user needs the authentication if the page is not terminated. This can expose administrative pages and allow the attacker to access vital information like list of users, their password

hashes or even create new users etc. This puts the attacker in pole position to carefully manipulate the website. This will put users at risk of their details being compromised.

### **LOGIN PAGE PASSWORD - GUESSING ATTACK**

This is another vulnerability exposed by the acunetix vulnerability scanner used to scan the sample mybooksandstationary.com. Login page password guessing is a type of attack vector deployed by attackers by trying out all possible password combinations with different usernames in a bid to log into a valid account. In other circumstances, login page password guessing is also known as a brute force attack. This attack is carried out successfully when the developer of the website has not specified a maximum number of login attempts to account holders on the website. Because the login attempts are left infinite and there is no lockout restriction, it gives room to attackers to comfortably try out their possible password combinations in the login page of the website countless times until they are successful. The possible combinations are made up of numbers, symbols and letters. Another login page password guessing attack method is a dictionary attack where attackers use a set of often used words mostly in English to try and identify a user's password. This vulnerability on the website does not only put users at risk but the administrator of the website as well. Most attackers look out for the administrator's password combinations first before any other user; most of the times.

### **POSSIBLE RELATIVE PATH OVERWRITE**

Possible relative path overwrite is another low vulnerability discovered by Acunetix vulnerability scanner. Relative path overwrite is a vulnerability in websites where target pages of relative urls (uniform resource locators) are overwritten by an attacker. Relative

path is a technique used by developers to link different pages on the same website without specifying the protocol e.g. http/https and the website's domain name. Relative paths are also used to link stylesheets, reduce the length of the website urls (uniform resource locators) also, for the pages to load within the same window than opening a new window which can be irritating to some users and to easily load files that are located in the same directory. However, attackers exploit vulnerabilities in this functionality and take advantage of websites like mybooksandstationary.com whose developers implement this functionality. Because browsers load the linked pages separately, attackers can frame malicious stylesheets and html pages which they control into the header of the website and trick browsers into loading them. With the possibility of this vulnerability present in the sample of study, it can result in users taking unintended actions like buying certain books or stationary they do not intend to buy, defacing the original style of the website and depending on how successful the attacker may be in exploiting this vulnerability, it could result in a cross site scripting attack. Because browsers interpret characters like backslash, comma, question mark etc. differently and also are not intelligent enough to determine right or wrong urls (uniform resource locators), attackers capitalize on such weaknesses in browsers to carry out relative path overwrite attacks. Even though a low vulnerability, it can frustrate patrons of mybooksandstationary.com to leave the website if every now and then they keep making unintended purchases which will cause the financial losses or realize they cannot enjoy the style of the website because a stylesheet might have been overwritten.

## **POSSIBLE SENSITIVE DIRECTORIES**

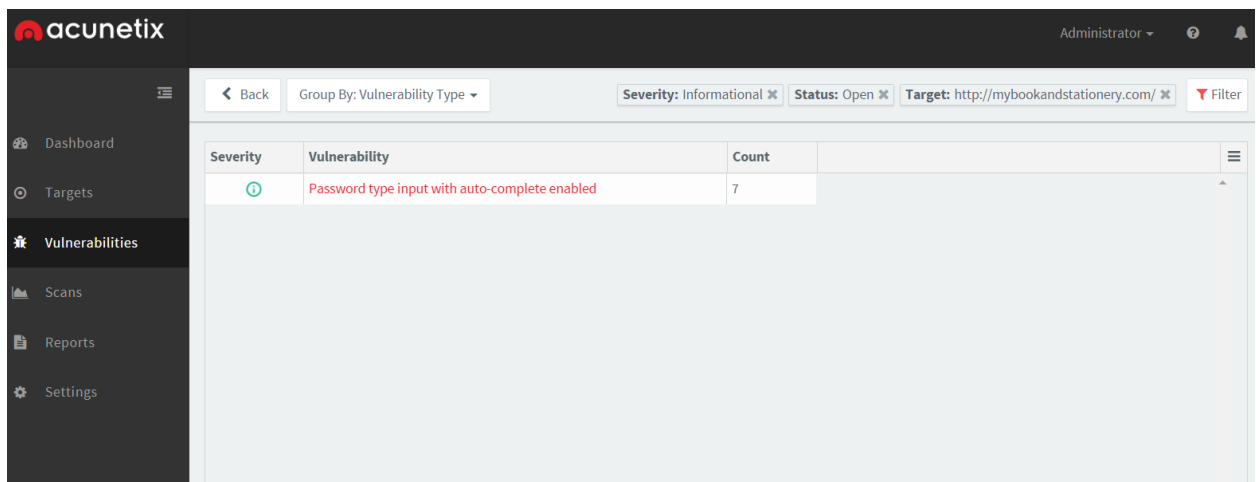
Findings from the acunetix vulnerability scanner shows that there are possible sensitive directories at risk with the sample domain. Directories are the folders in which files that render the website are stored and hence are very sensitive. Even though they are not directly linked from the website, it is a low possibility that resources like backup directories, database dumps, administration pages and other temporary directories may be vulnerable and attackers can use it to gather information about the website and frame more precise attacks. The presence of this vulnerability means that any successful exploitation of it by an attacker can make the attacker manipulate these directories by injecting malicious files which can compromise an entire sensitive directory like the backup directory.

## **POSSIBLE SENSITIVE FILES**

Sensitive files are files that contain certain sensitive information which should otherwise be hidden. After scanning the sample; mybooksandstationary.com with Acunetix vulnerability scanner, it is revealed that, there is a low possibility of sensitive files existing in the website. When developers do not restrict access to such files or completely remove them from the website, this vulnerability is possible. Some of these sensitive files could be password files, configuration files, log files, database dumps etc. This vulnerability can aid a malicious user with intentions of attacking the domain to gather information from this files and frame more advance and precise attacks which will exploit the website. The presence of this vulnerability puts legitimate users at risk of their user unique information like passwords and usernames being disclosed or used for some malicious activity by any attacker who successfully exploits it. Files like the database

dumps which contain information about table structures and some instances include data from the table and password files which store passwords could be a treasure in the box for an attacker who is able to access this files. Leaving this vulnerability open will only help attackers exploit the domain and cause more harm than good.

## ACUNETIX WEB VULNERABILITY SCANNER SNAPSHOT



The screenshot shows the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes the Acunetix logo, a user dropdown (Administrator), and a notification bell. Below the navigation bar, there are filters for Severity (Informational), Status (Open), and Target (http://mybookandstationery.com/). A table displays the results of the scan, showing a single vulnerability: 'Password type input with auto-complete enabled' with a count of 7. The table has columns for Severity, Vulnerability, and Count.

Severity	Vulnerability	Count
Informational	Password type input with auto-complete enabled	7

Figure 4. Informational Vulnerabilities. Source: Acunetix Web Vulnerability Scanner version 11.

## PASSWORD TYPE INPUT WITH AUTO-COMPLETE ENABLED

This vulnerability is a type of vulnerability where an attacker with local access to a user's computer can exploit. The sample; mybooksandstationery.com has an auto complete feature where usernames and passwords are auto-completed so long as they bear resemblance to any username and password which has been used to log onto the website and is saved in the browser cache. The browser asks users on their first login if they want to save their credentials or not. This feature possess great risk because anyone with local access to an original customer's system can make a purchase from the website using the customer's credentials on his or her blind side. Even though the developers



might have activated the feature to make login easier for the website patrons, it has a high potential of causing them some financial loss.

## **FINDINGS ON MYBOOKSANDSTATIONARY.COM BY OBSERVATION**

By observation at the premises of mybooksandstationary.com, the study has observed that, the website owners run a closely knitted working environment with three web developers. They all work on the same projects most times by dividing the project into modules and using modular programming approach to get the project done. After getting the desired product; the website, each has an access to the control panel of the hosting account where the website will be hosted by using common password for each of the developers to upload his codes via a file transfer protocol (FTP) connection to the host at his own convenience. This is done on a mutual agreement and trust of each other that, they will keep the common password safe and sacred. This can be a major breach point of the website since none of the developers can totally guarantee the safety of the password with the other.

It has also been observed that, the developers at mybooksandstationary.com do not consult any information technology security expert to proofread and analyze their codes before deploying them to the host for onward publishing of the website. So long as the codes behave as the developers want and they get the desired outcome, it is deployed without checking for any vulnerabilities that might be embedded in the lines of codes.

It has also been observed that, even though the web developers at mybooksandstationary.com have their own internet connection to the office via a broadband, they do not have any other security mechanisms aside a strong password on the router to ensure that data transmitted over the broadband connection is secured and free from any sniffing attempts given that, the development is to bring out a unique

product and any successful interception attempts could result in a competitor rendering a similar page.

## **FINDINGS ON MYBOOKSANDSTATIONARY.COM FROM A SEMI-STRUCTURED INTERVIEW CONDUCTED**

- **What is security to a web developer?**

As web developers, security means a lot of things to us and we take it seriously because without that, our toils for months can be brought down in a second and we do a lot of research to get our security right.

- **What cyber security considerations do you take note of when developing the website?**

Some of the considerations we considered as developers is the encryption of data and possible cyber-attacks that the website can be vulnerable to. We cannot trust the user therefore, we need to consider as much possible considerations as we can.

- **Do you think of the consumers' safety or you are only concerned about the frontend?**

When it comes to websites, you are developing for a target and you must have the target in mind so definitely, we consider consumers in order to keep their details on transactional websites like mybooksandstationary.com confidential and safe.

- **Do the clients themselves care about cyber security?**

Yes, some do. Because it is a transaction website, some clients who visit are careful about their security so their confidential details like phone numbers, names, card details etc. are not intercepted by anyone.

**What does a web developer look for in a web host?**

As developers, the uptime of the host is important to us because we do not want our website to be offline and when users want to transact business they find it difficult and also if the hosting company has a good record of cyber security resilience, provide 24hr client support during downtime.

- **Does breaches of content management systems scare you as a developer?**

It does not bother or scare us much because they are big companies and anytime there has been a vulnerability exploitation, they quickly release patches both manual and automatic to rectify the problem.

- **What will be your first reaction to a hack on your domain?**

We leave everything taking our attention and check where and how the hack came about. Whether it was an error on our part or from the hosting company. This is the first step in troubleshooting the hack.

- **What are some of the errors that can result from you?**

Maybe we have not properly escape some strings or validated some fields which have created loophole for the attack to happen.

- **What are some of the errors that can result from the web host?**

If their database is compromised and usernames and passwords of hosting accounts has been accessed by the attackers, they can access the file transfer protocol (FTP) files of the host's client and delete websites.

- **Do we take cyber security seriously in Ghana? Both consumers and companies.**

Ghana does not operate a vibrant e-commerce environment on the web. People barely use their bank card i.e. credit or debit cards to buy from the internet and companies also do not suffer from cyber-attacks as other companies in other countries do so they are relaxed on security especially cyber security.

- **How well can your domain resist a hack attempt?**

It depends on which type of attack it is. No one can tell what an attacker is thinking so it is difficult to tell how well the domain can resist a hack attempt. What we do is to make sure we sanitize the codes and hope no one tries anything funny.

- **How can you protect your website against malverts?**

Because malverts are generated from the advertising companies and is executed on the client's browser, there is not much we can do. Rather, the client has to be alert and careful on which adverts they click and must make sure their computers are well protected with up to date antiviruses, activate add blockers in the browsers to weed out some of these possible attacks.

- **Do you have a password policy in company?**

We do. We advise a strong password of alphanumeric combination and also keeping the password safe from everyone else. The password is what unlocks you and gives you permission on the network and so any activity executed from a system is presumed to be

done by the user of that system so we try to keep it safe as much as possible and also strong.

- **What about the shared passwords of the hosting accounts?**

The shared passwords of the hosting account during production is immediately changed by the one leading the project after the other developers are done uploading their files via the file transfer protocol.

- **How do you handle inactive accounts on the domain?**

We set a threshold on the accounts to check their activity or inactivity. A threshold of six months. If the account has not been used in the last six months for any transaction on the website, the account is suspended for another six months and when there is still inactivity on the same account it is completely deleted.

- **What in your opinion is a strong login credential?**

A weird username and a password of alphanumeric and space combinations. If the client tries the normal guesses like age, birthdate, social security number etc., they might be vulnerable to brute force attacks.

- **Are you abreast with current security trends and threats?**

As developers yes. Knowing the current trends and threats will help us keep up and update the website to stay in line with current developments.

- **Public and private web hosting, which do you prefer?**

Private hosting may be more secured but it is expensive managing a private facility. A lot of resources is needed e.g. utility and personnel but with the public you pay for a space and all these are done. They offer additional client support and all that so we prefer a public host than hosting the website privately.

- **Do you have any security procedure you follow when developing the domain?**

Yes. We make sure we escape strings properly, do the proper field validations, and encrypt data like usernames and passwords that are transmitted through the website.

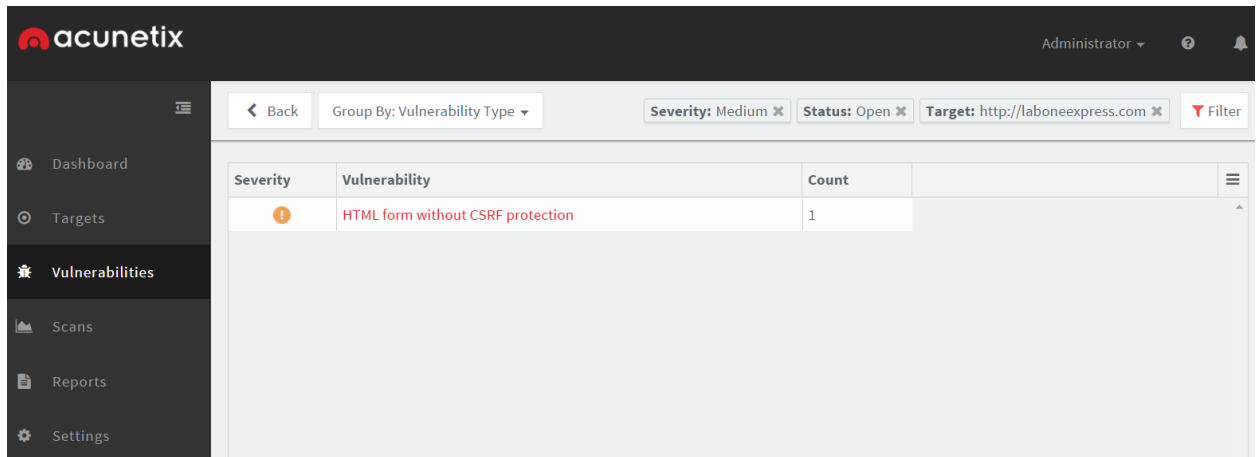
- **Finally, do you test the domain for vulnerabilities?**

Yes. We do we try to test the website occasionally using tools like acunetix vulnerability scan software to see if there are bugs and how we can fix them.



## FINDINGS ON LABONEEXPRESS.COM USING ACUNETIX WEB VULNERABILITY SCANNER

### ACUNETIX WEB VULNERABILITY SCANNER SNAPSHOT



The screenshot displays the Acunetix web interface. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main area has a top navigation bar with the Acunetix logo, user 'Administrator', and a notification bell. Below this is a filter bar with 'Back', 'Group By: Vulnerability Type', 'Severity: Medium', 'Status: Open', 'Target: http://laboneexpress.com', and a 'Filter' button. The central table lists vulnerabilities with columns for Severity, Vulnerability, and Count. One entry is visible: a medium severity issue titled 'HTML form without CSRF protection' with a count of 1.

Severity	Vulnerability	Count
Medium	HTML form without CSRF protection	1

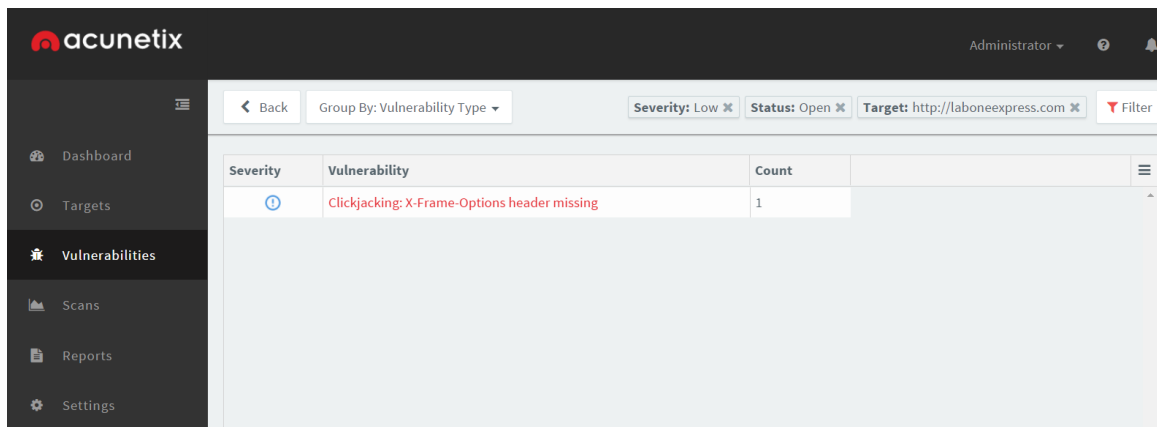
Figure 5 Medium Vulnerability. Source: Acunetix Web Vulnerability Scanner version 11.

### HTML FORM WITHOUT CSRF PROTECTION

According to Acunetix vulnerability scanner which was used by the study to scan the sample, laboneexpress.com has a medium level vulnerability of an html form without csrf (Cross Site Request Forgery) protection. Csrp (Cross Site Request Forgery) is a state changing attack vector. Because the attacker cannot benefit from data retrieval, csrf is focused on changing state requests like transferring funds from bank accounts and attacks on social media accounts. Csrp (Cross Site Request Forgery) is mostly exploited with html and Javascript. The sample; laboneexpress.com, has an html form which accept comments from users after every story on the page. This form allows users who wish to make a comment identify themselves by their email, name or social media identity on

social networking sites Facebook, twitter and google+. With the presence of a csrf vulnerability with the form, attackers who might be enraged with the opinion of another user can frame a task specific url (uniform resource locator) from their own constructed malicious website and lure the victim through social engineering abilities into running the url (uniform resource locator) to execute tasks like submitting an opinion which contradicts the victims original opinion, or a self-defamatory comment with the victim's identity. The attackers can frame the form with their opinions beneath an image on the malicious website and set the values as hidden. This leaves the victim clueless and less suspicious of any attack. However, this can sway the argument about a particular topic on the website and the victim's credibility of expressing valid opinions could be compromised. Because labonnexpress.com is a website where people interact with the webmaster and other readers, there is likelihood of difference in opinions and intolerance among some readers therefore, such a vulnerability does not better the situation.

## ACUNETIX WEB VULNERABILITY SCANNER SNAPSHOT



The screenshot displays the Acunetix Web Vulnerability Scanner interface. The top navigation bar includes the Acunetix logo, a user profile dropdown for 'Administrator', and a notification bell. The left sidebar contains a menu with 'Dashboard', 'Targets', 'Vulnerabilities', 'Scans', 'Reports', and 'Settings'. The main content area shows a filter bar with 'Back', 'Group By: Vulnerability Type', 'Severity: Low', 'Status: Open', 'Target: http://labonnexpress.com', and a 'Filter' button. Below the filter bar is a table with the following data:

Severity	Vulnerability	Count
Low	Clickjacking: X-Frame-Options header missing	1

Figure 6 Low Vulnerability. Source: Acunetix Web Vulnerability Scanner version 11.

## **CLICKJACKING**

This is a vulnerability which has been exposed by the Acunetix vulnerability scanner use to scan the sample laboneexpress.com. Clickjacking is a vulnerability where malicious codes are framed underneath buttons on legitimate websites to convince the user into thinking that, they are performing a particular action whereas what actually happens is that, they are directed to another page they do not intend visiting. Attackers use this type of attack vector to direct users to a page they believe they have already been authenticated on and perform malicious activities with the users' privilege. They can also be framed to deploy Trojans and malwares on the users' computers in a bid to vandalize data or to lockout the computer for a ransom. This attack can be used to achieve many ends, like tricking users to like and share pages and posts on Facebook, follow someone on twitter, click on google AdSense ads for pay per click revenues etc. Attackers use legitimate websites like the sample; laboneexpress.com with such vulnerabilities to trick readers into performing these undesired actions. Laboneexpress.com does not have any X-frame Options header implementation which means that, the http header has no specification on whether or not pages should be hosted or embedded in an iframe element. This vulnerability can be capitalized on by any attacker who finds it and will use it to exploit laboneexpress.com patrons. Patrons of the sample are not safe with this vulnerability lurking in the codes.

## **FINDINGS ON LABONEEXPRESS.COM BY OBSERVATION**

By observation at laboneexpress.com, the study has observed that, the website is administered by one individual who builds and maintains the website. The individual has no other web developer offering assistance and he tends to administer the website on the go, anywhere there is an internet connection; public or private access in order to get contents on the website for patrons on time. As a result, the pressures of development can make him loose site of errors in the codes which can result in a vulnerability which can be exploited by attackers to attack the website.

It has also been observed that, because the developer manages the website on the go and careless about what type of connection over which he is accessing the internet, the developer could log onto a public connection over which attackers might be sniffing data and that could be a breaching point which can be used by attackers to disorganize the codes and work done could be zilch. Even with private connection, the developer, has no extra security on the internet broadband access except a strong password in order to guard against any data sniffing attacks.

It has also been observed that, the web developer at laboneexpress.com does not contact any information technology security expert to proofread and analyze the codes for errors and vulnerabilities. So long as the codes work as thought, it is deployed to the host for publishing on the website.

## **FINDINGS ON LABONEEXPRESS.COM FROM A SEMI – STRUCTURED INTERVIEW CONDUCTED**

- **What is security to a web developer?**

To me as a web developer, security is about securing my files and folders and online properties to prevent unauthorized access and use.

- **What cyber security considerations do you take note of when developing your website?**

I consider all possible cyber security threats that can affect my website and alter the data on it. Especially on the administrator account and other user accounts like editors and contributors.

- **Do you think of security when developing your website?**

Yes. I think of security in the context of risk to the website. I do that in the sense that, it is an intellectual property and people also do advertise on it through pay per click adds so in order to secure my income stream, I have to think of how secured the product will be.

- **Do your readers worry about being possibly exposed to cyber-attacks?**

No, not any that I know of. But I make the effort to ensure that it is safe for readers by installing scam control plugins and other security plugins provided by my content management system provider.

- **Which content management system do you use?**

I use WordPress.

- **Does breaches of content management systems scare you as a developer?**

Well, it does not scare me but it raises concerns. Concerns to the extent that, how will the breach affect my operations.

- **What will be your first reaction to a hack of your domain?**

Based on my knowledge, my first reaction will be to try and restore my website in order to continue servicing clients who want to access content on the website.

- **Do you backup your website?**

Yes I have a backup for the website content. I don't use these automated backups because it consumes the space I have on the website and I need more space so, I just download the sql databases which include all the media files, comments, articles and all, zip it and later upload to my google drive.

- **How well can your domain withstand a hack attempt?**

Because the website runs on WordPress, WordPress core files are usually updated with security patches so I make sure I regularly update them to the latest versions and so I can say the domain is quite robust. The website has been up for six years now and there has been no hack incident recorded.

- **What other user accounts are on the website?**

Contributors. They are those who want to write articles and publish on the website so with them, I create an account for them to allow them upload their articles.

- **Do you use any form of encryption?**

No. I don't use any encryption on the website.

- **Foreign and local host which do you prefer?**

I prefer a foreign host to a local host because they are more reliable and respond promptly to requests. So far they have been good. I don't know any local hosting company too so probably they do not market themselves well enough.

- **How are you likely to handle any vulnerability exposed by the study?**

I will investigate the vulnerability first, and then, proceed to contact an information technology consultant for advice and take action afterwards.

- **Finally, do you test your domain for vulnerabilities?**

No. So far, I have not run any test on the domain for any vulnerability.

## **CHAPTER 5**

### **5.1 INTRODUCTION**

The fifth chapter of the study presents summary, conclusion and recommendation. This chapter also points to the limitation of the study and provides suggestions for further areas of research.

### **5.2 SUMMARY**

The research identifies vulnerabilities exploitable by cyber attackers, the types of attacks websites are susceptible to, the extent of damage a successful exploitation of the susceptibilities can cause the organization, prevention and mitigation measures available and the challenges in implementing them and best approach website administrators should take to keep their websites safe. The objective/intention is to draw administrators to the reality of cyber-attacks, explore the effects cyber-attacks on websites have on patrons and to serve as a learning curve to other administrators and organizations about cyber-attack prevention and mitigation on their websites.

The study adopted a qualitative research methodology, non - probability sampling, primary and secondary sources of data collection and a deductive analysis of the data obtained.

The study revealed findings on two websites; mybooksandstationary.com and laboneexpress.com through Acunetix vulnerability scanner, observation and semi-structured interviews. The Acunetix vulnerability scanner grouped the findings into different categories depending on their severity i.e. high, medium, low, and informational level vulnerabilities.



### 5.3 CONCLUSION

The study has made useful findings of attacks on websites using two different websites as case study. The high vulnerabilities are critical vulnerabilities that must be fixed immediately to prevent any severe damage to the website and its users in the event of an exploitation attempt. A successful blind sql injection will modify the websites database by bloating it with unwanted data or deletion of vital data critical to the functioning of the domain. Databases at the backend of the website is the most valuable resource of the website and compromising it will have a devastating effect on both domain owners who will have to spend substantial amounts of their income in cleaning the database and recovering it while assuring users of the confidentiality of their details in the midst of the chaos and users who will want to access the domain for legitimate reasons may either be served with wrong information or have their confidential details such as usernames, passwords, emails and phone numbers in the custody of a malicious third party who is likely to trade those details for financial gains.

Sql injection even though has a different approach of exploitation has the same resulting effects of a blind sql injection attack.

Cross site scripting is another high level vulnerability the study has revealed in the findings. Cross site scripting is used to exploit the user directly by inserting scripts into the client side url (uniform resource locator) which are executed in the users browser to redirect them to a phished website designed by the attacker to draw in users to login in with their credentials which will then be sent to the attackers' server or transmit browser specific information like cookies and session tokens to the attackers. A successful exploitation of this vulnerability on mybooksandstationary.com will result in the

website's patrons loosing confidence in purchasing from the website since they are not guaranteed a safe transaction and confidentiality of their details and transaction records. However, the users will always find an alternative by moving their demands to a more secured domain or resorting to the traditional methods of buying their books and stationaries. The result of this on the website will be a loss in revenue and market share and this will affect how competitive they will be in the e-commerce market space.

The medium vulnerabilities are those vulnerabilities that fall between the high and low vulnerabilities of the findings by Acunetix vulnerability scanner. The medium level vulnerabilities also pose a risk to the smooth functioning of the websites and must be fix sooner than later. Vulnerabilities like the application error messages which are generated automatically by system in the event of an unhandled exception are sources of information to an attacker as the error messages could include file location and other file details. Backup files that are on the website is also a wrong practice that can be properly leveraged by an attacker to attack the website. The backup is clone copy of the original domain and contain useful information which should be secured. Files within the backup must not be accessible by any other party. Html form without CSRF (cross site request forgery) protection will allow attackers to create forms on malicious websites that mimic forms on the original websites and frame attacks beneath those forms with the original domains as targets. This will result in users performing unintended actions on the target websites. This will result in customers seeking alternative websites where they can be intentional in their actions and not be tricked.

User credentials are personal identifiable information which uniquely identify every user therefore, transmitting them in plaintext is dangerous. Any attacker who intercepts the

connection to the web server and traverses through the files and directories is likely to have access to the user details and will exploit them for financial gains to the detriment of both users and the website.

Javascript libraries which are no more useful to the functioning of the websites must be taken out of the codes that render the current design of the website. Because, old JavaScript libraries which are not in use but are existent in the codes can be exploited by attackers to deploy payloads that can result in cross site request forgery.

Low vulnerabilities are those flaws that pose the least risk to the website. Even though this vulnerabilities are low, considering the dynamism with which attackers carry out attacks on websites in recent times, these flaws must be treated with urgency like any other severe vulnerability by the website administrators of the websites studied. Vulnerabilities like login page password guessing attack should not take the administrator much to fix. Because there is no threshold set on the number of login attempts, attackers can deploy vectors like dictionary attack on users in order to find login credential combination of users and exploit them.

A successful attempt will exploit the user however, the website will be most affected because they might have to pay all affected users some compensation and also spend some more in rectifying the vulnerability. Clickjacking vulnerability existent in the sampled websites where attackers can frame malicious codes beneath buttons to lure users into performing unintended actions can lead to a mistrust of the domains by the users and cause them move their demands to a more secured and trustworthy website.

Possible relative path overwrite can cause attackers to overwrite a whole directory of the website with their own data and this can compromise the integrity of information on the website. Possible sensitive directories and files that have been revealed by the Acunetix vulnerability scanner as low vulnerabilities pose a risk as any successful exploitation of these vulnerabilities which contain files like database dumps, administration pages, and backup directories etc. could benefit the attacker to frame more precise and concise attack payloads to destruct normal functioning of the website.

Informational vulnerability is a vulnerability that must be taken notice of and corrected before it is exploited and becomes a high, medium or low vulnerability. Password type input with auto-complete enabled is an informational vulnerability. Even though it is to make the login for users on mybooksandstationary.com easier, users who share their computers or the device they use to login will be at risk as anybody in custody of the device can login to their accounts with the help of the password type auto-complete feature and make purchases in their names. This will cause financial loss to the user.

It was discovered that, access to the control panel where the ftp (file transfer protocol) connection is established for publishing of the website is shared by all developers who work in group at mybooksandstationary.com. This practice is a risk to the website because, none of the developers can guarantee the safety of the credentials which is also used by the other developers to render the page. Any loose handling of the control panel credentials by any of the developers or a social engineering tactics employed by an attacker against any of the developers will result in a direct access of the control panel by the attacker.

The study also revealed that, the samples studied do not engage information technology security professionals to analyze their source codes, proofread them and fix any bugs that may be existent before they are published.

Broadband connectivity is important. However, administrators are not conscious of security mechanisms except strong passwords to prevent sniffing of data packets which could result in a competitor sniffing data packets containing source codes and manipulating it to their benefits. Administrators are also loose in choosing what type of connection the logon to i.e. public or private.

However, administrators know that in the cyberspace, there are a lot of risks which they are susceptible to and each of the administrators at the samples studied maintain some level of security procedures in production and after production to keep their domains safe. This however is not sufficient. Cyber security is a process not an event, and with the dynamism of attackers and sophistication of attacks, building an attack resistant domain, administrators must move beyond their personal security check lists and look at the bigger picture of vulnerabilities, how to prevent them and leverage the opportunities of a secured domain to attract more internet users and increase their market share.

From the findings it has been revealed that, the ecommerce website mybooksandstationary.com has more vulnerabilities than the magazine website laboneexpress.com. This means that, mybooksandstationary.com is likely to suffer more attacks and spend more on securing the domain than laboneexpress.com.

## **5.4 RECOMMENDATION**

The study recommends the following for implementation by the websites studied as a solution to the vulnerabilities that the study has revealed.

The study recommends that, user inputs should be properly sanitized by validating input fields which require users' input. Users must input exactly what is required of them into the input fields and any different input should be rejected. Also, developers should use parameterized sql queries and stored procedures in the construction of the databases, limit the privileges of other database users to their environment only. This will prevent and mitigate the risk of sql and blind sql injection vulnerabilities.

Encoding untrusted html and JavaScripts and converting them into safe outputs and displayed back to the user as data without executing them in the browser and properly escaping and validating inputs will help prevent and mitigate cross site scripting vulnerability.

Developers should properly handle exceptions by writing another set of codes to perform a desired function in the event that the main function fails. This will prevent the system from generating its own error messages which could reveal file locations and other basic sensitive information as an error message.

Backup files which are stored in directories of the website accessible over the web must be removed from such directories to prevent attackers from accessing the backup at the least exploitation.

Html forms on the samples studied without csrf (cross site request forgery) protection must implement csrf protection measures by reviewing the html form codes and make the

website generate a cookie value for the forms each time a user interact with the forms and require the cookie value in the submission of every form to authenticate that the actions being performed by the user is intended and not triggered by an attacker on a malicious website.

User credentials which are sent in clear text into the database must be encrypted. User credentials are personal identifiable information and must be protected. Encryption of these credentials can be done by implementing an https (hypertext transfer protocol secure) connection on the website to automatically encrypt data and transmit to the database.

Vulnerable JavaScript libraries which exist within the codes of the website must be permanently removed to avoid any exploitation by an attacker. Any Javascript library that is no more in use to render the current state of the website must be removed from the set of codes that render the current state of the website.

The vulnerability of clickjacking can be prevented by specifying an X-frame option header to prevent attackers from embedding the contents of other websites in frames or iframes of the sample websites. The X-frame option header options could be deny; which completely denies any attempt to embed a file into the frame or iframe, same-origin; which allows the page loaded in the iframe or frame to be displayed by the same website and finally allow from uri; which allows the website to load its iframe or frame with a trusted domain. Specifying one of these options i.e. deny, same-origin and allow from uri will avoid the vulnerability of clickjacking.

Account lockout policies must be developed to lockout users of mybooksandstationary.com after a number of unsuccessful attempts at logging into their accounts. This will prevent the login page password guessing attack vulnerability.

Possible sensitive directories and files which contain sensitive data such as database dumps, password files, log files, configuration file etc. which have the capability of providing an attacker with information must be removed from directories which are accessible over the web to prevent giving an attacker sensitive knowledge about the website.

Password input type auto-complete which allows password inputs to be auto-completed at the users end must be disabled to avoid malicious individuals who have local access to a user's computer from logging into their accounts and making purchases.

The study further recommends that, services of information technology security experts should be sought by the websites studied to proofread their source codes to identify errors and fix the necessary bugs which developers might have lost sight of. Engaging this professionals to sanitize the code will also improve the quality of the final product i.e. the website.

In situations where developers need to work in group and upload files via the FTP (file transfer protocol) to the control panel, the study recommends that, the main account owner should be the one to upload the files and not share the control panel username and password with the other team members to upload files at their own convenience. This is recommended to keep the control panel login credentials secured since its security cannot be guaranteed with many individuals. One individual should be responsible for it.



To prevent an attacker from sniffing data packets over their broadband connections at the office, the case study should add additional security measures than only a strong password. They should disable the SSID (service set identifier) broadcast to prevent their wireless name from displaying on other nearby computers connection list to prevent it catching the eye of an attacker who might need an internet connection and will want to exploit it, enable MAC (media access control) address filtering where only trusted computers are allowed access to the connection and disable administrative access to the router through the web and any configuration changes they desire to make to the router should be done locally by connecting an ethernet cable from the computer to the router.

It is also recommended that full backups are taken of the websites current state and stored on a different webserver and should be often tested to determine whether they can function as desired during any eventuality of the main domain breaking down. Regular vulnerability tests should also be run on the websites using vulnerability scanners like Acunetix Web Vulnerability Scanner to expose existing vulnerabilities and fix them immediately they are found out. Keeping them only increases the chance of exploitation.

There is no single best approach for website administrators to take in keeping their domains and patrons safe rather, a sum total of the little cyber security procedures which they must keep is what can help keep their domains and patrons safe.

Finally, administrators and developers of the websites studied should endeavor to be abreast of cyber security threats which are associated to websites and constantly upgrade their skills to keep their domains and patrons safe.

## **5.5 LIMITATIONS OF THE STUDY**

The study is a case study which has employed a qualitative research methodology, as a result, the findings are most relevant to the websites studied; mybooksandstationary.com and laboneexpress.com. Therefore, generalizing the findings without further research could produce inaccurate results.

## **5.6 SUGGESTION FOR FURTHER STUDIES**

Since the scope of the study is to identify cyber-attacks websites are susceptible to and the prevention and mitigation measures website administrators can take to keep their websites and patrons safe, further studies can be done on how website administrators respond to fixing the vulnerabilities which have been detected on their websites.

## **APPENDIX**

### **SEMI – STRUCTURED INTERVIEW GUIDE**

1. What is security to a web developer?
2. What cyber security considerations do you take note of when developing?
3. Do you think of customers' safety or you are only concerned with the frontend?
4. What will be your first reaction to a hack of your domain?
5. What are some of the errors that can result from you?
6. How well can your domain resist a hack attempt?
7. Do your readers worry about being possibly exposed to any cyber-attack?
8. Does breaches of content management scare you as a developer?
9. Do you backup your website?
10. Do you use any form of encryption?
11. Do you test your domain for vulnerabilities?

## REFERENCES

- Acunetix. (2015). *Acunetix web application vulnerability report*. Acunetix.
- Acunetix. (2016). *Acunetix web application vulnerability report 2016*. Acunetix .
- Bershad, J. (2011, May 10). *Report: Computer Hackers Have Stolen And Leaked Fox Broadcasting Emails And Passwords*. Retrieved December 2, 2016 , from Mediaite: <http://www.mediaite.com/online/report-computer-hackers-have-stolen-and-leaked-fox-broadcasting-emails-and-passwords/>
- Cluely, G. (2014, September 22). *eBay XSS password-stealing security hole "existed for months"*. Retrieved November 26, 2016, from Graham Cluely: <https://www.grahamcluley.com/ebay-password-stealing-security-hole-existed-months/>
- Ebay. (2014, may 21). *eBay Inc. To Ask eBay Users To Change Passwords*. Retrieved november 23, 2016, from ebay: <https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords/?>
- IBM. (2016). *IBM X-Force Threat Intelligence Report*. IBM.
- IBM. (2016). *IBM X-Force Threat Intelligence Report 2016*. IBM.
- Imperva. (2015). *Imperva 2015 web application attack report* . Imperva Inc.
- Mirkinson, J. (2011, July 31). *PBS Hacked Again By LulzSec In Retaliation For WikiLeaks Documentary*. Retrieved November 26, 2016, from Huffpost: [http://www.huffingtonpost.com/2011/05/31/pbs-hacked-again-by-lulzs\\_n\\_868941.html](http://www.huffingtonpost.com/2011/05/31/pbs-hacked-again-by-lulzs_n_868941.html)
- Ponemon Institute. (2015). *2015 Cost of Data Breach Study: Global Analysis* .
- Practical Law Company. (2011). *Cyber Attacks: Prevention and Proactive Responses*. New York: Practical Law Publishing Limited and Practical Law Company, Inc.
- Seetharaman, J. F. (2014, May 27). *Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees*. Retrieved November 23, 2016, from Business Insider: <http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5?IR=T>
- Symantec. (2008). *Symantec Internet Security Threat Report Trends for July–December 07*. Symantec corporation .
- Westaway, L. (2011, June 3). *Sony hacked again, with over one million users' details nicked*. Retrieved November 25, 2016, from Cnet: <https://www.cnet.com/news/sony-hacked-again-with-over-one-million-users-details-nicked/>
- Whitehat Security. (2016). *Whitehat Web Applications security statistics report 2016*. Whitehat Security Inc.